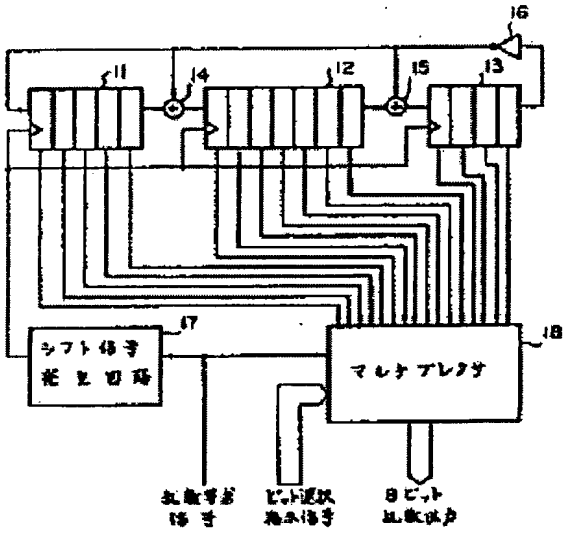
PSEUDO RANDOM NUMBER GENERATOR

Patent number:	JP1258130
Publication date:	1989-10-16
Inventor:	AOKI MASAO
Applicant:	MATSUSHITA ELECTRIC IND CO LTD
Classification:	
- International:	G06F7/58; H03K3/84
- european:	
Application number:	JP19880085385 19880408
Priority number(s):	JP19880085385 19880408

Abstract of **JP1258130**

PURPOSE:To generate pseudo random number sequence having uniformity with a high level and to perform logical analysis by generating the same pseudo random number repreatedly by enabling the pseudo random number to be generated only by a shift register having a fly-back circuit.
CONSTITUTION:When a random number request signal is generated, a shift signal generation circuit 17 generates a shift signal, and changes the output values of shift register circuits (11-13) by shifting via exclusive OR circuits 14 and 15 and an inversion circuit 16. A multiplexer 18 receives the output of 16 bits of the shift register circuits (11-13), and selects eight bits by a bit selection indication signal and outputs them as a random number. In such a way, it is possible to generate the pseudo random number having the uniformity with the high level with simple constitution, and to generate the same pseudo random number repeatedly, and to perform the logical analysis.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1−258130

⑤Int. Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)10月16日
G 06 F 7/58		C−7056−5B	
H 03 K 3/84		A−8626−5J	

審査請求　未請求　請求項の数 1　(全4頁)

㊹発明の名称　擬似乱数発生装置

㉑特　願　昭63−85385
㉒出　願　昭63(1988)4月8日

㉒発明者　青木　正夫　神奈川県横浜市港北区綱島東4丁目3番1号　松下通信工業株式会社内
㉑出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代理人　弁理士　星野　恒司

明　細　書

1．発明の名称　擬似乱数発生装置

2．特許請求の範囲

排他的論理和回路と反転回路または排他的論理和回路のみによって構成される帰還回路とシフトレジスタから成る符号系列発生器と、乱数要求の発生時に上記シフトレジスタのシフト信号を発生する制御回路と、上記シフトレジスタの出力する複数ビットのうちの一部のビットをビット順はそのまま、または入れ換えて出力する演算回路とを備えたことを特徴とする擬似乱数発生装置。

3．発明の詳細な説明

（産業上の利用分野）

本発明は確率モデルによる解析や、シミュレーション等を実行する装置、乱数を利用したプロトコルを実現する通信制御装置、乱数を利用する暗号生成装置およびゲーム機等に使用する擬似乱数発生装置に関する。

（従来の技術）

従来、この種の擬似乱数発生装置は（特開昭61−163435号公報に記載されているように）第3図に示すように構成される。第3図において、31は一定時間間隔で出力値を増加させる自走カウンタ、32は自走カウンタ31の出力値を記憶する一時記憶回路、33は一時記憶回路32に記憶された内容を乱数として出力する出力回路である。

次に上記従来例の動作について説明する。第3図において、自走カウンタ31は外部信号に関係なく常に一定間隔で出力値が増加している。乱数要求信号が発生すると、そのときの自走カウンタ31の値を一時記憶回路32に格納する。出力回路33は、一時記憶回路32に格納された複数ビットの数値のうち、一部のビットあるいは全ビットを取り出して乱数として出力する。

このように、上記従来の擬似乱数発生装置でも、乱数要求信号が自走カウンタ31が出力値を増加する時間間隔より十分大きな時間間隔で非周期的に発生すると擬似的に乱数を発生させることができる。

（発明が解決しようとする課題）

しかしながら、上記従来の擬似乱数発生装置では、乱数要求信号の発生する時間によって乱数値が決定するため論理解析することが不可能であり、理想的な乱数を必要とする用途には使用できないという問題があった。また、同一の擬似乱数列を繰り返して発生させる必要のある場合にも使用できなかった。本発明はこのような従来の問題を解決するものであり、簡易な構成でありながら自然乱数に近似した擬似乱数を発生し、同一の擬似乱数列を繰り返して発生できるようにすることで、論理的解析を可能にした優れた擬似乱数発生装置を提供することを目的とするものである。

（課題を解決するための手段）

本発明は上記目的を達成するために、排他的論理和回路と反転回路または排他的論理和回路のみによって構成される帰還回路とシフトレジスタから成る符号系列発生器と、乱数要求の発生時に上記シフトレジスタのシフト信号を発生する制御回路と、上記シフトレジスタの出力する複数ビットのうち一部のビットをビット順はそのまま、または入れ換えて出力する演算回路とを備えたものである。

（作　用）

本発明は上記のような構成により次のような作用を有する。すなわち、乱数要求信号が発生すると制御回路がシフトレジスタにシフト信号を出力し、シフトレジスタの内容を帰還回路を通してシフトさせることによって上記シフトレジスタの出力値を変える。この出力値は一様乱数に近い性質を持つため、さらに一部のビットをビット順はそのままあるいは入れ換えて出力する回路を通すことによって、高度の一様性を持つ擬似乱数にすることができる。また、シフトレジスタの初期値を同じ値にすることによって、同一の擬似乱数列を発生することができるという効果を有する。

（実施例）

第１図は本発明の一実施例の構成を示すものである。第１図において、11，12，13はシフトレジスタ回路であり、排他的論理和回路14，15および反転回路16からなる帰還回路によって非最長系列発生器が構成される。17はシフト信号発生回路、18はマルチプレクサである。

次に上記実施例の動作について説明する。上記実施例において、乱数要求信号が発生するとシフト信号発生回路17がシフト信号を発生し、シフトレジスタ回路11，12，13を、排他的論理和回路14，15と反転回路16を通してシフトさせることによってシフトレジスタ回路11，12，13の出力値を変える。マルチプレクサ18はシフトレジスタ回路11，12，13の出力16ビットを受けとり、ビット選択指示信号によって８ビットを選んで乱数として出力する。上記のように、本実施例によれば16ビットのシフトレジスタの値のうち８ビットのみ出力するため、生成される擬似乱数列の周期は非常に長くなるという利点を有する。また、ビット選択指示信号によって出力するビットとその順序を選択できるため、いろいろな擬似乱数列を発生させることができる。

第２図は本発明の他の実施例の構成を示すものである。第２図において、21，22，23，24はシフトレジスタ、25，26，27は排他的論理和回路、28はシフト信号発生回路、29はレジスタである。第２図の実施例では16ビットのシフトレジスタと３つの排他的論理和回路を用いてｍ系列発生器を構成している。さらに16ビットのシフトレジスタの出力のうち８ビットのみを用いているため、全ビットが０を含めて取り得るすべての値を最大の65535の周期で出力できるという利点を有する。また、本実施例では、シフトレジスタ21，22，23，24の出力を乱数要求信号の発生直後にレジスタ29に記憶させている。したがって、乱数要求信号発生時に次回の出力値をレジスタに記憶させておくため、乱数要求信号が発生するとただちに乱数が出力できるという効果を有する。

なお、上記実施例では８ビットの乱数を生成しているが、乱数のビット数は特に制限はない。したがって、更に長周期の擬似乱数を出力する擬似乱数発生装置または上記実施例より回路の小さな擬似乱数発生装置を得ることができる。

（発明の効果）

本発明は上記実施例より明らかなように、以下に示す効果を有する。

(1) 擬似乱数列を帰還回路を持つシフトレジスタのみによって発生しているので、簡易な構成の論理回路によって擬似乱数発生装置を実現できる。

(2) 再現性を有さない物理現像や乱数要求信号の発生する時間間隔を利用していないので、同一の擬似乱数列を繰り返して発生させることができる。

(3) 同一の擬似乱数列を繰り返して発生できるので、論理的解析が可能であり、目的に合った性質を持つ擬似乱数列を発生できる装置を設計することができる。

(4) 簡易な論理回路によって構成しているので、乱数要求信号が生じるとただちに乱数を発生することができる。

4. 図面の簡単な説明

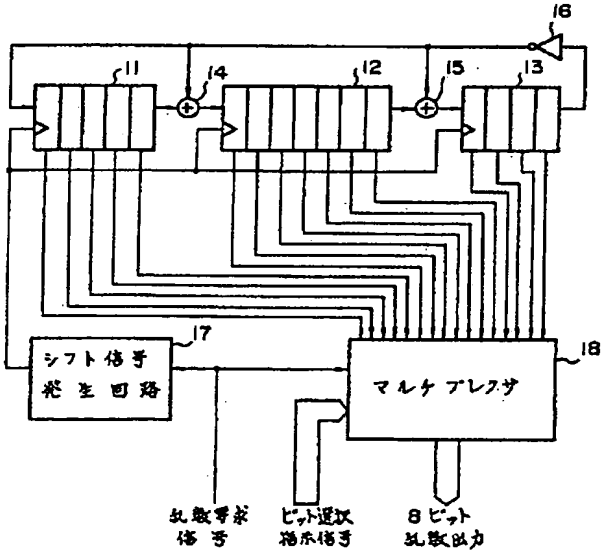
第1図は本発明の一実施例を示す擬似乱数発生装置の概略機能ブロック図、第2図は本発明の他の実施例の擬似乱数発生装置の概略機能ブロック図、第3図は従来の擬似乱数発生装置の概略機能ブロック図である。

11,12,13,21,22,23,24 … シフトレジスタ、14,15,25,26,27 … 排他的論理和回路、16 … 反転回路、17,28 … シフト信号発生回路、18 … マルチプレクサ、29 … レジスタ、31 … 自走カウンタ、32 … 一時記憶回路、33 … 出力回路。

特許出願人　松下電器産業株式会社

代　理　人　　扇　野　恒　司

第1図

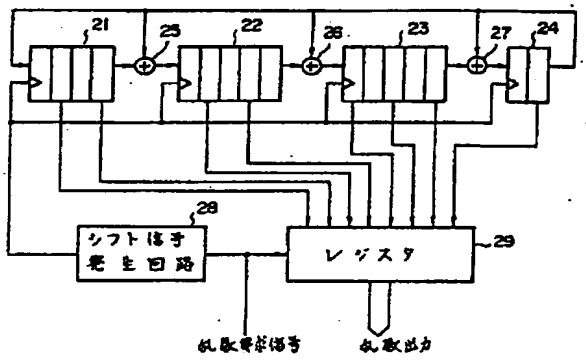


11, 12, 13 … シフトレジスタ回路

14, 15 … 排他的論理和回路

16 … 反転回路

第2図



21, 22, 23, 24 … シフトレジスタ回路

25, 26, 27 … 排他的論理和回路

第 3 図